Password Processing Scheme using Enhanced Visual Cryptography and OCR in Hybrid Cloud Environment

Ranjith.R, Supreeth S, Ramya R, Ganesh prasad. M, Chaitra Lakshmi L

Abstract— to authenticate the user using the password can be achieved by simply converting the password into the values is called hash. Even though there are many websites which can unlock the hash values by using some cracking tools called as cyber attacks. This cyber attacks are very much common by the way of hacking the passwords by hackers. Hackers can undeniably figure out the plain text using such software's it gives n-number of examples of plaintext samples which the hackers can execute and crack open or penetrate into personal information in the Hybrid Cloud Environment. To overcome this type of trouble or mishap our system is recommended. The proposal is that our system not only converts the plaintext into hash values but it will be stored as an image, the user will only be having an ID and login password (at the time of user creation) . The user when he wants to login he will receive an email in which a share-1 image will be present which is encrypted completely even he himself can't be able to recognize what it is, the server will ask him to download the share-2 image then he has to enter his user ID for the server to recognize his User-ID. Since these images are encrypted both share images 1&2 are encrypted by VC (Visual Cryptography) then the user has to merge these two images, if it matches then only the user can login. This merge method undergoes OCR (0ptical cryptography recognition). Our aim is to prevent hackers from gaining access to personal information of the users in Hybrid Cloud Computing Environment.

Keywords—Visual cryptography, Optical Character Recognition (OCR), Hybrid Cloud Computing

I. INTRODUCTION

The normal process through which the user authentication takes place by considering a hash-based scheme by verifying the password and their user-id in order to verify the password In hash-based password scheme the plain text password is converted into hash value by the hashing function [10]. Computational velocity is fast and it is easy to process. In most of the system this scheme is been practiced in many system. Because it is just text and the hash functions used in this method are very quick. But this type of authentication is very easy to be cracked and illegally used by the hackers they use some attacks like run dictionary based attack or brute force attack by password cracking tools or some hash cracking sites which is available online [11]. Assume that someone has a password using their own name example "john" if he gets to know this he can easily get to the hash value then he easily crack it. Attackers can easily guess what kind of hash function is been used in the system. Even though the attacker doesn't know any information about the hash value or password. Due to all these problems we need to think about a new solution to the problem. In this regard a image based password encryption scheme can be applied so that the system can be protected safely by using Visual Cryptography and Optical Character Recognition (OCR). In this paper it is clearly emphasized on the implementation of VC & OCR technique to adopt in Hybrid cloud computing environment [12]. Because especially in Hybrid Cloud Computing Environment password authentication is a big a challenge. In Hybrid Cloud computing environment password is stored in Private Infrastructure and storing of Data is done at the public infrastructure. So there is a chance of hacking in switching between Private infrastructure and Public infrastructure for while using their system.

II. RELATED WORK

As hash functions can be easily understood and also what kind of function is used could be found out by the attacker. By this system can be damaged by the attacker. The user himself is responsible for such attacks. In a particular research many people were inquired about the password management functions. Many such systems with different function and with resistance from attacks have been proposed. Many users have chosen plain-text to hash value password encryption to overcome complexity. We have proposed a system which converts plain-text to hash in the form of image which will be encrypted. Add the procedure how he logs in and receives image and all same things.

The user has to login to get to the user account he should login with a password since plaintext and hash value can be easily decrypted by the attackers ,even though there are many such text based or hash value based systems are available none of them are safe and prominently efficient.

A. Hybrid Cloud Computing

In [13] Cloud-to-Edge system authentication has been discussed and implemented Instant message Protocol

Revised Manuscript Received on April 25, 2019.

Ranjith.R, School of C&IT, REVA University, India.
Supreeth S, School of C&IT, REVA University, India.
Ramya R, School of C&IT, REVA University, India.
Ganesh Prasad. M, School of C&IT, REVA University, India.
Chaitra Lakshmi L, School of C&IT, REVA University, India.

(IMP) and it provides good performance in the middleware layer. This which does not affect the performance of the whole System. But in this approach a new method of authentication can be introduced to strengthen the key to protect from the hackers.

In [14] explores the different Security issues are addressed in a multi-tenant environment for many businesses that affect the Cloud Computing. In this paper author has mentioned some general issues of Cloud Environment.

In [15] the author has emphasized on Resource allocation and load balancing aspects. But author has failed to work on security aspects of Cloud Computing to address the issues of data security.

B. Visual Cryptography

In [16] Visual Cryptographic technique has been implemented by dividing the 4 shares in a two stage approach. But the Author can improvise by adopting Visual Cryptography followed by different cryptographic technique to improvise the key.

C. Optical Character Recognition

In [17] Author has contributed a hash based Image decipherment with the scheme called Optical Character Recognition. As a result, it can verify extracted Saved-ID by comparing with Client-ID. But Author has not compared with previous existing algorithms for comparison.

III. METHODOLOGY

The complete process of handling the sequence of the Authentication System is as follows.

1. The user inputs the user ID and password.
2. The system of the user creates a image with text. If the saved image exists on user's device, it does not have to create the image again.
3. The system constructs the second image by considering original image. Since the system does not possess the first shared image. Because the device already knows to construct the first shared image.
4. The client sends the second shared picture just to the server.
5. The server consolidates the main shared picture and the second shared picture received.
6. The server must decrypt the merged image as to get the original image.
7. By using OCR scheme, ID is been retrieved using decrypted image.
8. The server authenticates the extracted ID is similar to original ID and it returns confirms whether the extracted ID is similar to the original ID and returns the Boolean value by verifying both.
9. If the server returns true then the user can login successfully.

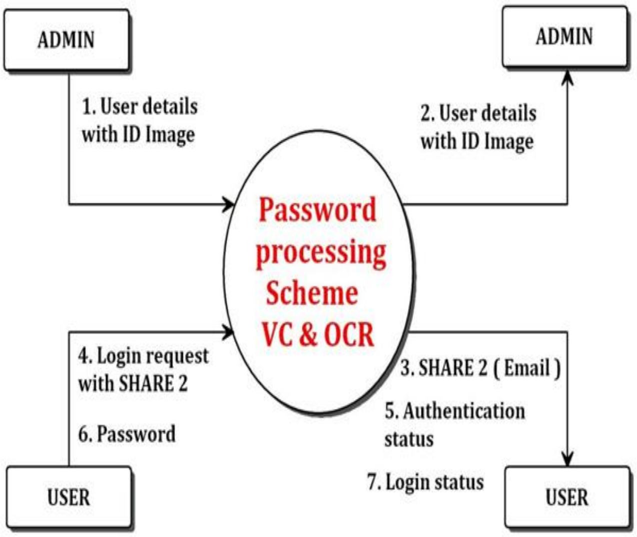

ADMIN
ADMIN
1. User details with ID Image
2. User details with ID Image
Password processing Scheme VC & OCR
4. Login request with SHARE 2
6. Password
3. SHARE 2 (Email)
5. Authentication status
7. Login status
USER
USER

fig 1: Module design

1. Halftone Visual Cryptography:

Shares of random binary patterns are generated by visual cryptography by encoding the Secret binary Image (SI). Here the meaningful binary images are converted into the shades. The binary patterns of the shares have no visual meaning and hinder the objectives of visual cryptography. But the visual quality of the shared images is poor. So In this paper, a technique named halftone visual cryptography is proposed to achieve visual cryptography via half toning based on the Figure 1.a.

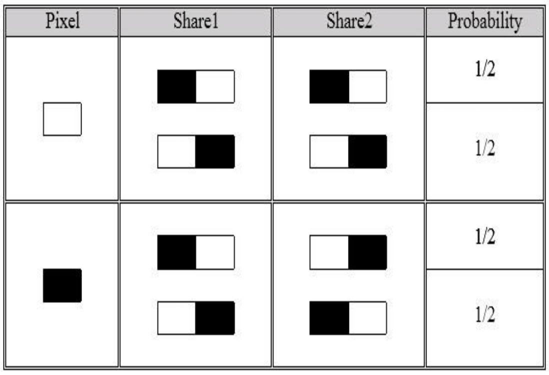


Figure 1.a: Visual Cryptography sharing scheme

Proposed method uses void and cluster algorithm [2] to encode the binary image into halftone shares carrying out significant information based on the blue-noise dithering principles [18]. The simulation shows that the visual quality of the proposed method is better than any other Visual Cryptographic methods.

2. OCR (optical character recognition)

Conversion of images of typed, handwritten, photocopy of a document or printed text is converted into machine-encoded text is called as Optical Character Recognition (OCR). This involves scanning of photos to analyze the text characters present in the image character by converting into character codes such as ASCII. Then

Computer easily recognizes the character codes such as ASCII commonly used in data processing.

OCR is used in many different fields like pattern recognition, computer vision and artificial intelligence. Older versions of OCR were needed to be trained with images of each character and work on one font only. But now days we are capable of producing high recognition accuracy for most fonts are now able to recognize from a variety of digital image file formats. The shares are generated by using visual cryptographic scheme and it is merged to form an image. In this paper OCR Scheme is been used for extracting the plain text from merged image. This plain text is matched with the plain text of image which is been converted from the image which is already present in the database. The Procedure of OCR is as follows:

Cleanup-up Phase: In this phase variety of technique is used to remove low-quality scans and to remove any blurs to make the OCR process as accurate as possible. The contrast is adjusted and text is sharpened.

The First Pass: Most of the modern OCR schemes operate on a two-pass principle. This means the first pass is processed without any previous knowledge of the document. This method scans commonly occurring symbol, breaks them down into their basic shapes and picking the letters then, start building of characters as a library.

The Second Pass: Then by using internal dictionary letters are guessed. The best OCR scheme is capable of checking for the grammar by scanning the document. and usage of sentence. By this at least a reasonable accuracy can be expect.

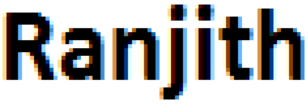


Fig 2: text image

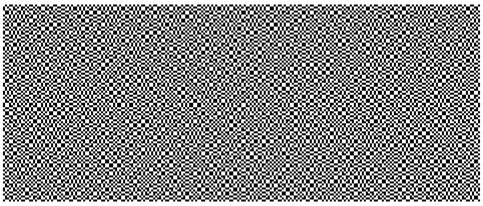


Fig 2.a: share1 image

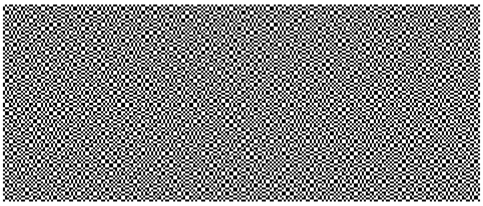


Fig 2.b:share2 image

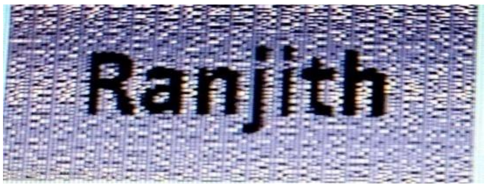


Fig 2.c: Final merged and decrypted image

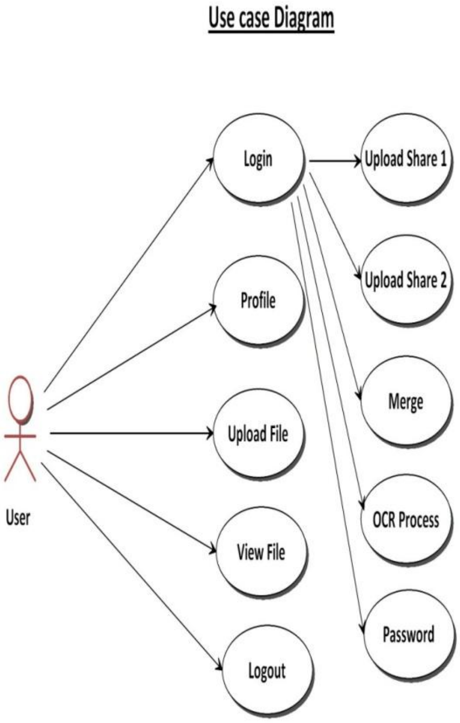


Fig 3: use case diagram of the user

This image shows the things which the user interacts with the elements of the system.

DATAFLOW DIAGRAM

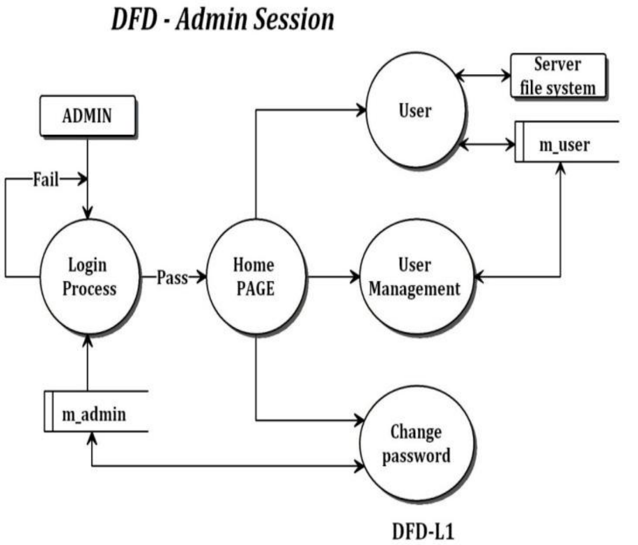


Fig 4.a: Data flow diagram of admin session

In the admin side the admin is the main [erson who logins into the system creates the user manages the users he has all the authority.

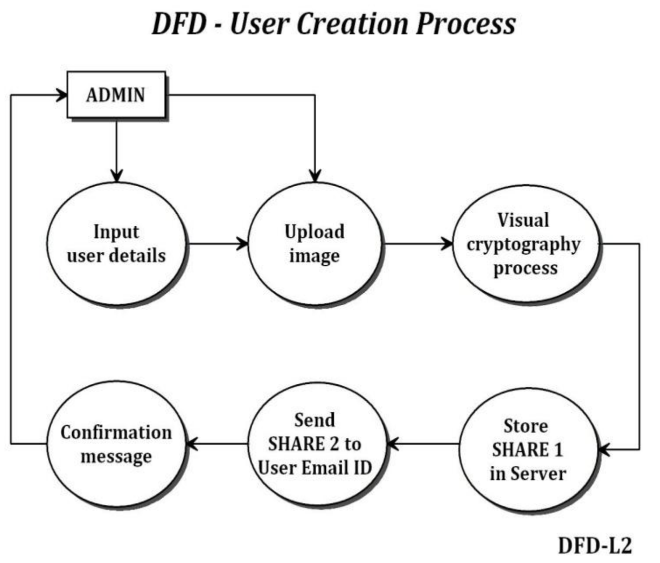


Fig 4.b: data flow diagram of user creation process

The user will be created by the admin he will input there details and upload a password image then the visual cryptography process will take place the share1 image will be the saved in the server and the share2 image will be sent to the user email id the user can download the share1 while login.

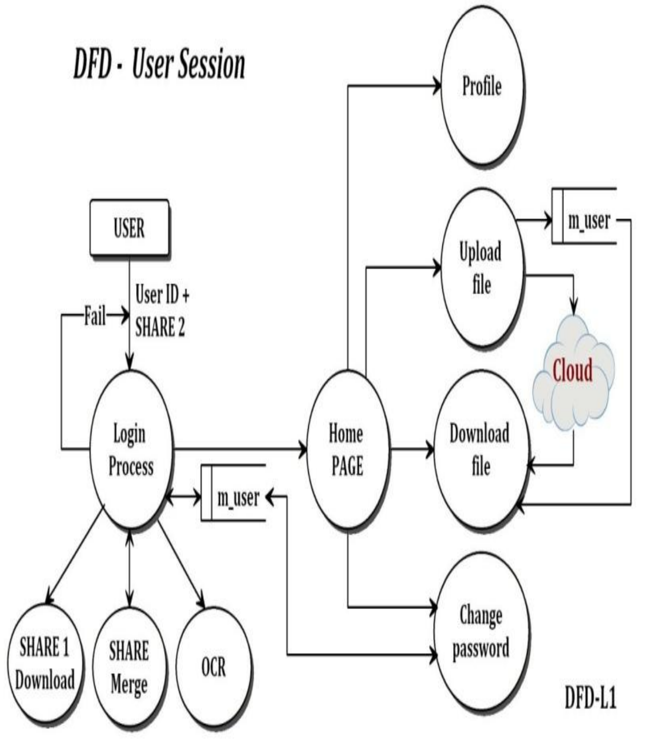


Fig 4.c: data flow diagram of user session

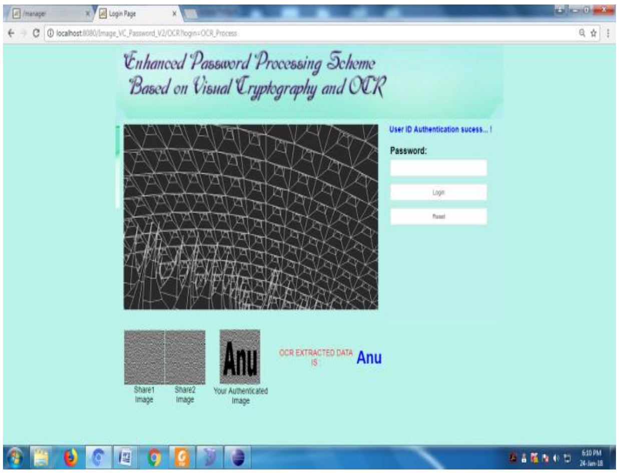
In the user session the user will provide the user id and share2 image sent to his mail and if it is correct he can download the share1 image and then the visual cryptography will merge the images and the OCR [4] will decrypt the image and it will recognize the text if it is correct then the user can give the process and login and go to home page.

Results and Discussion

Our project has few benefits compared to the old password processing techniques .The first one is we are using image instead of plain text, second we are using visual cryptography instead of text-based hash and finally we are using OCR for identifying the data present in the image and validates it whether it's the same or not based on this our project has the following advantages:

- better security
- lower chances of hackers to hack your account
- privacy of the user data

When the user inputs the user id and upload both the share1&2 images the visual cryptography and OCR process takes place.


/manager
Login Page
localhost:8080/Image_VC_Password_V2/OCR?login=OCR_Process
Enhanced Password Processing Scheme
Based on Visual Cryptography and OCR
Login
Reset
Anu
Share1 Image
Share2 Image
Your Authenticated Image
6:10 PM
24-Jan-18

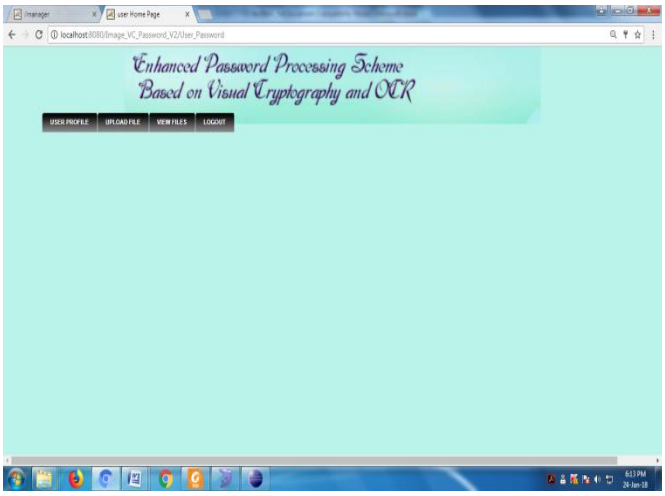
User ID Authentication sucess...!

Password:

OCR EXTRACTED DATA IS Anu

Fig 4.c: Authentication process in the project

Once the authentication is done the user inputs the password and logs in successfully .Then he will go to the user page .That is shown in the next diagram.


/manager
user Home Page
localhost:8080/Image_VC_Password_V2/User_Password
Enhanced Password Processing Scheme
Based on Visual Cryptography and OCR
USER PROFILE
UPLOAD FILE
VIEW FILES
LOGOUT
6:13 PM
24-Jan-18

The user logs into the system more securely without lot of trouble he has his privacy even if anyone gets the share2 image they can't login because they don't know the user id and the password at the end of the login process.

CONCLUSION

Most of the people do not give a strong and secure password they are not having the knowledge of how to set a password. Even though they bought up different ideas like checking the password before the user sets it and checks whether the password is of desired of length and even they tried to check whether password s present in a set of similar and common password used by password cracking tools it is still a problem to safeguard the account from cyber attacks. So we have used encrypted image by halftone visual cryptography which splits the image into two parts and then it merges it and use OCR to check the character present in the image and validate it to login so it is strong compared to the old password schemes. This approach which can help in managing the password scheme in Hybrid Cloud computing.

REFERENCES

1) Naor, M. and A. Shamir. Visual cryptography, Advances in cryptology. Eurocrypt ’94 Proceeding LNCS, 950:1–12, 1995.

2) Everitt, Brian Cluster analysis. Chichester, West Sussex, U.K: Wiley. ISBN 9780470749913, 2011.

3) Silva, Vladimi, "Practical Eclipse Rich Client Platform Projects (1st ed.)". Apress. p. 352. ISBN 1-4302-1827-4, March 2009.

4) Riedl, C.; Zanibbi, R.; Hearst, M. A.; Zhu, S.; Menietti, M.; Crusan, J.; Metelsky, I.; Lakhani, K. (February 20, 2016). "Detecting Figures and Part Labels in Patents: Competition-Based Development of Image Processing Algorithms". International Journal on Document Analysis andRecognition. 19 (2):155.

5) Gaw, Shirley, and Edward W. Felten, "Password management strategies for online accounts," Proceedings of the second symposiumon Usable privacy and security. ACM, 2006.

6) Nguyen, Thi Thu Trang, and Quang Uy Nguyen, "An analysis of Persuasive Text Passwords, "Information and Computer Science (NICS), 2015 2nd National Foundation for Science and Technology Development Conference on. IEEE,2015.

7) Tam, Leona, Myron Glassman, and Mark Vandenwauver, "The psychology of password management: a tradeoff between security and convenience, "Behaviour & Information Technology 29.3 (2010): 233- 244.

8) Wang, Luren, Yue Li, and Kun Sun, "Amnesia: A Bilateral Generative Password Manager," 2016 IEEE 36th International Conference on Distributed Computing Systems.

9) Gauravaram, Praveen, "Security Analysis of salt‖ password Hashes,"Advanced Computer Science Applications and Technologies(ACSAT),2012 International Conference on. IEEE, 2012.

10) Christoforos Ntantogian , Stefanos Malliaros , Christos Xenakis, " Evaluation of Password Hashing Schemes in Open Source Web Platforms", Computers & Security, Volume 84, July 2019, Pages 206-224.

11) VidyaRao, PremaK.V."Light-weight hashing method for user authentication in Internet-of-Things", Ad HocNetworks, Volume 89, 1 June 2019, Pages 97-106.

12) XunYi, ZahirTari, FengHao, LiqunChen, Joseph K.Liu, XuechaoYang, Kwok-YanLam, IbrahimKhalil, Albert Y.Zomaya" Efficient threshold password-authenticated secret sharing protocols for cloud computing", Journal of Parallel and Distributed Computing, Volume 128, June 2019, Pages 57-70.

[13] Antonio Celesti, Maria Fazio, Antonino Galletta, Lorenzo Carnevale Jiafu Wan, MassimoVillari, " An approach for the secure management of hybrid cloud–edge environments", Future Generation Computer Systems, Volume 90, January 2019, Pages 1-19

[14] P. Ravi Kumar, P. Herbert Raj , P. Jelciana, "Exploring Data Security Issues and Solutions in Cloud Computing", 6th International Conference on Smart Computing and Communications, ICSCC 2017, 7-8 December 2017, Kurukshetra, India.

[15] S Supreeth, Shobha Biradar, "Scheduling virtual machines for load balancing in cloud computing platform", Int. J Sci Res, Volume 2, Issue 6, pp. 437-441,06/2013.

[16] Mr. Rohith S, Mr. Vinay G, "A Novel Two Stage Binary Image Security System Using (2,2) Visual Cryptography Scheme", International Journal Of Computational Engineering Research, May-June 2012 | Vol. 2 | Issue No.3, pp.642-646.

[17] Nazia Nusrath Ul Ain, Meena Kumari K S, Mujaseema Kahnum, "Password Authentication Using Image Decipherment And Ocr", International Journal Of Innovations In Engineering Research And Technology [Ijiert], Volume 5, Issue 3, Mar.-2018

[18] Iliyan Georgiev , Marcos Fajardo, Blue-noise dithered sampling, ACM SIGGRAPH 2016 Talks, July 24-28, 2016, Anaheim, California

AUTHORS PROFILE

Mr.Ranjith R pursuing Bachelor of Technology in Computer Science and Engineering from Reva University, Bangalore in 2019.

Mr. Supreeth S holds M. Tech. degree in Computer Science and Engineering from Visvesvaraya Technological University, Belgaum. He has been a technology educator for two years, teaching various subjects like C Programming and Data structures, Software Testing, Finite Automata and Formal Languages, Virtualization and Cloud Computing, Cloud Architecture, Big data and Data analytics. He is interested in pursuing research in Cloud Computing. He has published many papers in International journals and presented in national conferences in the area of cloud computing, Big Data.

Ramya R, pursuing Bachelor of Technology in Computer Science and Engineering from Reva University, Bangalore in 2019.

Ganesh prasad.M, pursuing Bachelor of Technology in Computer Science and Engineering from Reva University, Bangalore in 2019.

Chaitra Lakshmi L, pursuing Bachelor of Technology in Computer Science and Engineering from Reva University, Bangalore in 2019.